



**CASE STUDY:**

A threat-led approach to cyber intelligence boosts efficiencies for global financial services provider

**INDUSTRY: FINANCE**

## About the client

The client is a multinational financial services provider with operations across North America and Europe. The organization manages critical digital infrastructure supporting millions of customers worldwide, including online banking, payment processing, and credit services. Operating in a highly regulated sector, the company faced increasing scrutiny around data protection, resilience, and compliance with financial regulations.

## The client's challenge

Despite significant investment in cybersecurity, the client's security teams remained largely reactive. Their reliance on open-source threat feeds and post incident analysis left them vulnerable to sophisticated adversaries. They often struggled to distinguish relevant threats from noise, which slowed decision-making and created blind spots. Key challenges included:

### Noise in threat feeds:

Large volumes of intelligence lacked prioritization and actionable context, resulting in wasted analyst time and missed opportunities for early intervention.

### Limited dark web visibility:

No systematic monitoring of leaked credentials, brand abuse, or stolen customer data exposed the organization to reputational and regulatory risk.

### Credential-based attacks:

Rising brute force attempts and phishing campaigns targeted both employees and customers, increasing the likelihood of unauthorized access and fraud.

### Evolving ransomware risk:

Sector wide increases in ransomware attacks threatened business continuity and compliance. According to recent industry data, the financial services sector remains one of the top three targets for ransomware groups globally.

### Lack of internal expertise:

Without a dedicated Cyber Threat Intelligence (CTI) function, the client could not fully analyze, contextualize, and disseminate relevant and prioritized intelligence across security and executive teams.

## Benefits

The CTI Tailored Threat Intelligence engagement delivered measurable outcomes within six months:



### Phishing campaign neutralized:

Fraudulent banking domains and a counterfeit mobile app were identified and removed within 48 hours of registration. Rapid takedown reduced the brand's phishing footprint by over 75% in that quarter, safeguarding customer trust and reputation.



### Credential exposure mitigated:

Monitoring uncovered thousands of leaked employee credentials, triggering a credential hygiene program that reduced the number of leaked credentials into the dark web by 90% brute force login attempts by 65% and hardened access controls across critical systems.



### Ransomware attempt disrupted:

Early detection of a BlackBasta ransomware campaign within 12 hours enabled rapid DFIR response, machine isolation, and prevented prevention of data exfiltration, with MTTR kept within 4 hours. The intelligence was quickly shared across teams, improving defenses against follow on campaigns.



### Operationalized intelligence:

CTI findings were directly integrated into SIEM enrichment, detection engineering, vulnerability management prioritization, and penetration testing exercises. This created a closed loop between threat intelligence and operational defenses.



### Improved executive visibility:

Monthly intelligence reports provided senior management with clarity on evolving risks, including emerging malware, ransomware activity, and geopolitical developments. These briefings elevated cybersecurity from an operational function to a board level priority.

Beyond operational outcomes, the client's leadership gained new confidence in its ability to demonstrate regulatory compliance and threat-led resilience to both regulators and customers. The proactive approach to CTI has positioned the organization as an industry leader in cyber defense maturity.

## Our solution

CyberProof deployed its Tailored Cyber Threat Intelligence (CTI) service, tightly integrated with the client's Security Operations Center (SOC), Digital Forensics & Incident Response (DFIR), and Vulnerability Management (VM) teams. The solution takes a threat-led approach, and combines advanced technology, analyst expertise, and agentic AI automation to deliver actionable, business specific intelligence that directly supported operational and strategic decisions in context.

Key service components included:

### Contextualized threat landscape intelligence:

Real time monitoring of global ransomware, malware, and phishing campaigns relevant to the financial sector. This intelligence was contextualized against the client's digital footprint, ensuring alerts were always relevant and prioritized.

**Asset-based intelligence:** Continuous monitoring of the client's domains, IP ranges, and brand Strategic threat advisory: Executive level briefings covering geopolitical risks, industry specific

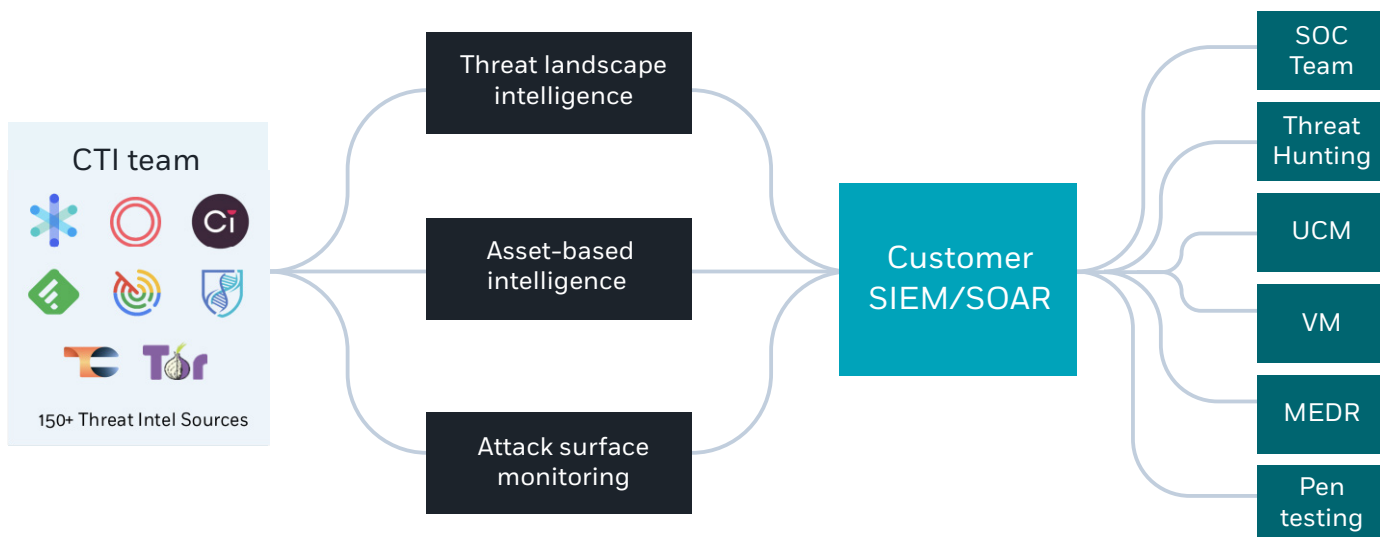
threat actor profiling, and MITRE ATT&CK aligned scenarios in the financial provider's context. These reports provided senior leadership with the visibility required to align security strategy with evolving business risk.

**Takedown services:** Rapid removal of fraudulent phishing domains, counterfeit mobile applications, and impersonation attempts that posed immediate risks to customers and brand reputation.

### Enhanced transparency and collaboration:

Clear visibility into how intelligence was collected, analyzed, and disseminated, ensuring integration across SOC, vulnerability, and red team functions. This strengthened cross-team collaboration and maximized the operational impact of the Cyber Threat Intelligence (CTI) team's outputs.

**Agentic AI integration:** AI agents automated data collection, profiling, IOC enrichment, and clustering. All outputs were validated by CyberProof CTI experts to maintain accuracy and eliminate false positives.



## Speak with an expert

Learn how CyberProof's [Tailored Threat Intelligence services](#) can help your organization strengthen its resilience against evolving cyber threats. [Book a meeting.](#)

## About CyberProof

CyberProof, a UST company, delivers better security operations and drives superior experiences for enterprise customers. Our cloud-first, AI-powered approach to security delivers industry-leading services to drive real business results. We believe that working closely with our customers and partners through a 'better security, together' services model jointly empowers us to defend against the greatest of threats. See: [www.cyberproof.com](http://www.cyberproof.com).

Barcelona | California | London | Singapore | Tel Aviv | Trivandrum